UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

Intellectual Ventures I, LLC, Intellectual Ventures II, LLC, Plaintiffs, v. Lenovo Group Ltd., Lenovo (United States) Inc., LenovoEMC Products USA, LLC, and EMC Corp., Defendants.	Civil Action No. 16-10860-PBS
Intellectual Ventures I, LLC, Intellectual Ventures II, LLC, Plaintiffs, v. NetApp, Inc., Defendant.	Civil Action No. 16-10868-PBS

MEMORANDUM AND ORDER ON CLAIM CONSTRUCTION

September 9, 2019

Saris, C.J.

INTRODUCTION

Intellectual Ventures I, LLC and Intellectual Ventures II, LLC (collectively, "IV") accuse Defendants EMC Corporation, Lenovo Group Ltd., Lenovo (United States) Inc., LenovoEMC Products, USA, LLC, and NetApp, Inc. (collectively "Defendants")

of infringing U.S. Patent No. 6,968,459 (the "'459 patent") entitled "Computing environment having secure storage device." IV asserts claims 15, 18, 24, and 25. Independent claims 15 and 18 state:

> 15. A method for accessing a storage device comprising:
>
> detecting a storage device within the storage drive;
>
> sensing whether a storage device has device-specific security information stored thereon;
>
> providing full-access to the storage device when the storage device has the device-specific security information by:
>
> encrypting digital data using the security information during a write access to write the digital data to the storage device; and
>
> decrypting digital data using the security information during a read access to read the digital data from the storage device; and
>
> providing restricted-access to the storage device when the storage device does not store the device-specific security information by preventing the digital data from being written to the storage device during the write access.
>
> 18. A method for controlling access to a storage device comprising:
>
> detecting a storage device within a storage drive;
>
> sensing whether the storage device has security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user;

> configuring the storage drive to prevent write access to the storage device when the security information is not sensed; and
>
> configuring the storage drive to permit write access by encrypting digital data using the security information and writing the encrypted digital data to the storage device when the security information is sensed.

'459 patent, claims 15 and 18. The parties dispute the claim construction of five terms: (1) "detecting a storage device within a storage drive," including disputes around "storage device" and "storage drive," (2) "sensing whether a storage device has [device-specific] security information," (3) "device-specific security information," (4) "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user," and (5) "encrypting digital data using the security information." The Court held a non-evidentiary Markman hearing on April 24, 2019, and the parties submitted supplemental briefing afterwards.

BACKGROUND

The '459 patent relates to a method of creating a secure computing environment by "preventing the authorized user from using sensitive data in an unauthorized manner." '459 patent, col. 1, ll. 21-23. With "conventional security measures" prior to the invention claimed in the '459 patent, it was "very difficult to prevent an authorized user from appropriating

sensitive data by simply copying the sensitive data to a removable storage device such as a floppy diskette." Id. at col. 1, ll. 23-26. To address this issue, the inventors of the '459 patent developed a computing environment "in which a computer automatically operates in a secure 'full-access' data storage mode when the computer detects the presence of a secure removable storage device." Id. at col. 1, ll. 36-39. Alternatively, "[i]f the computer senses a non-secure removable storage device then the computer automatically operates in a 'restricted-access' mode." Id. at col. 1, ll. 39-42.

Figure 1 of the '459 patent, below, illustrates a system-level overview, depicting "a diagram of a computer 100 that automatically operates in a secure data storage mode when the computer 100 senses that storage device 151 is a secure storage device." Id. at col. 2, ll. 30-33. "Each storage device 151 represents a removable device having a storage medium for holding digital information such as a floppy diskette . . . ." Id. at col. 3, ll. 8-10. "Each removable media drive 121 represents a device suitable for servicing access requests for storage device 151 such as a floppy drive . . . ." Id. at col. 3, ll. 13-15.

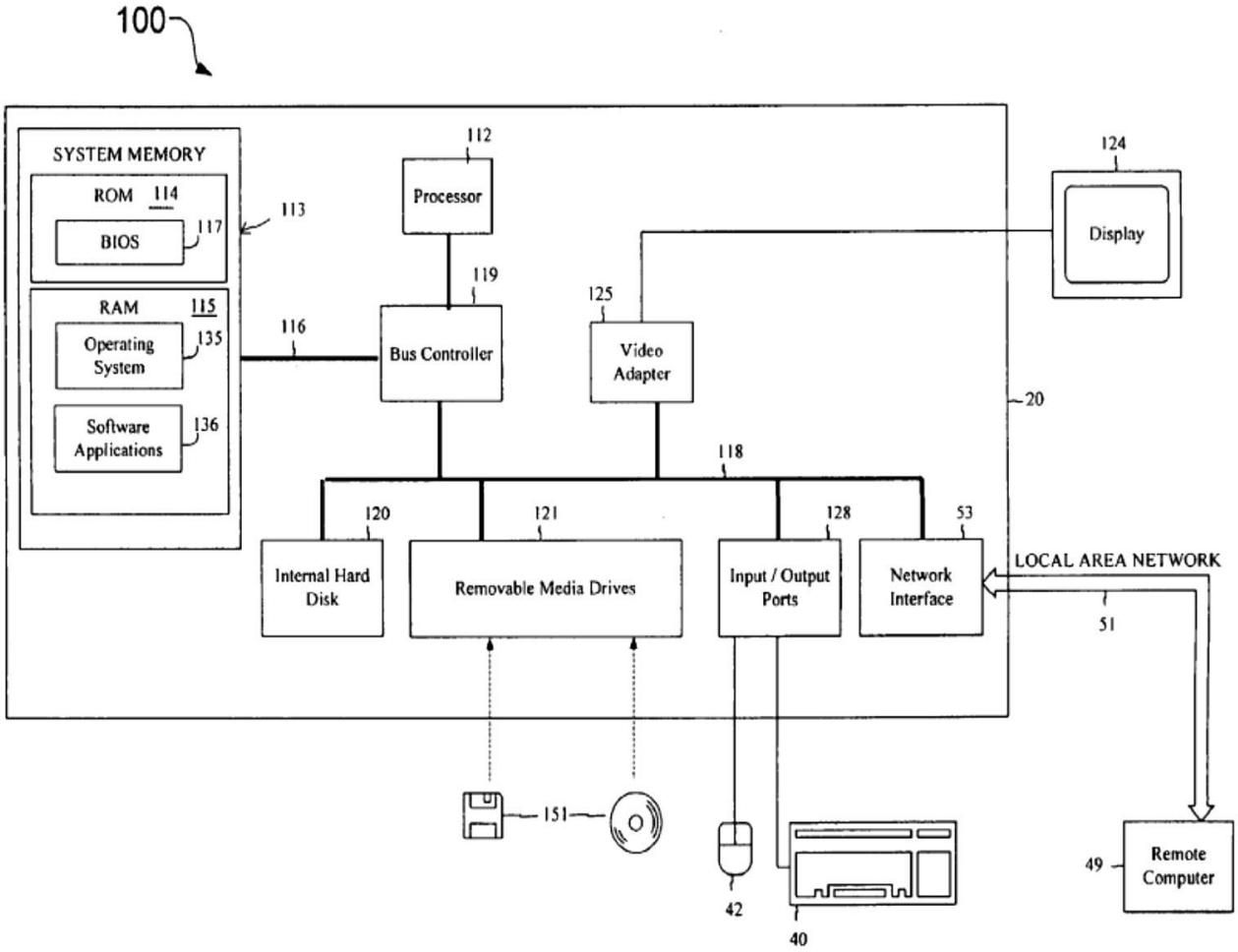


FIG. 1

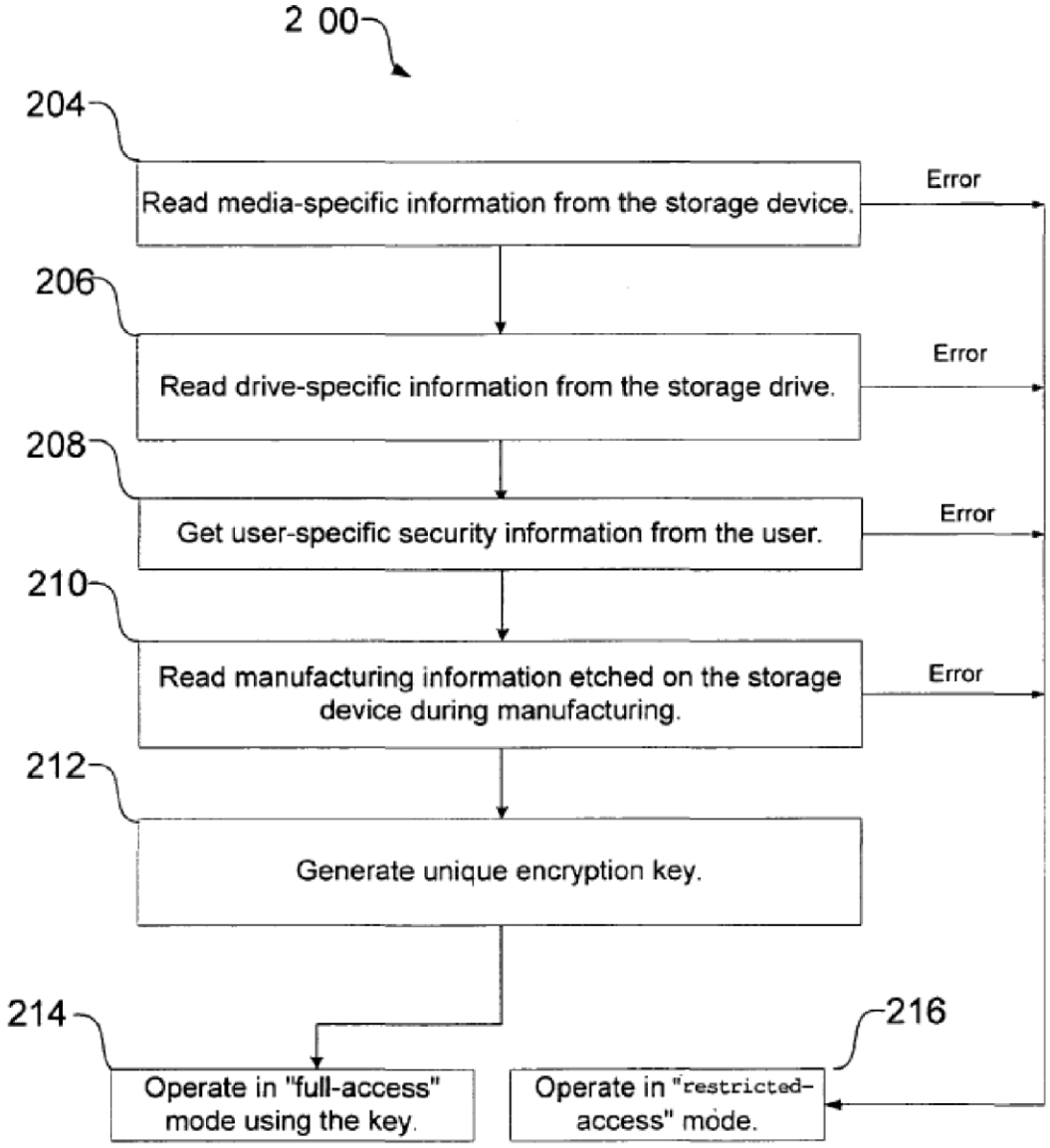
According to the invention, "computer 100 automatically operates in full-access data storage mode only when the computer 100 detects a secure removable storage device 151 present within any one of the removable media drives 121." Id. at col. 3, ll. 57-60. To "automatically detect whether a storage device 151 is a secure device, computer 100 determines whether device-specific security information was written to storage device 151." Id. at col. 4, ll. 6-9. Method 200, illustrated in the figure below,

details an exemplary way in which software applications 136 on computer 100 (hereinafter referred to as the "storage manager") detect the required security information to allow computer 100 to operate in full-access mode.[1] See id. at col. 4, ll. 46-52. "In block 204, the storage manager detects whether storage device 151 is a 'secure' removable device by attempting to read any device-specific security information from storage device 151." [2] Id. at col. 5, ll. 7-10. "In block 206, the storage manager retrieves drive-specific security information that is specific to removable media drive 121 such as a serial number or calibration parameters . . . ." Id. at col. 5, ll. 20-22. "In block 208, the storage manager retrieves user-specific security information from the computer user by, for example, prompting the user for a password, or performing a retina or fingerprint scan." Id. at col. 5, ll. 39-42. "In block 210, the storage manager retrieves manufacturing information that was physically

[1] "In one embodiment, the storage manager performs method 200 anytime a . . . storage device 151 is inserted into removeable media drive 121. In another embodiment, the storage manager performs method 200 at the request of a user." '459 patent, col. 4, ll. 57-62.

[2] "[I]n one embodiment the device-specific security information is a hash of the addresses of the bad sectors for storage device 151. Because it is a function of the physical characteristics of the actual storage medium within storage device 151, the format information is inherently unique to each storage device 151." '459 patent, col. 4, ll. 12-17. "In other words, the addresses of the bad sectors change from device to device." Id. at col. 4, ll. 18-19. This seems like cataloguing where a specific floppy disk or CD is scratched or damaged such that the specific portion of the removeable storage device could not have data written on to it, or read from it, in those areas.

etched on storage device 151 during the manufacturing process." Id. at col. 5, ll. 47-49.[3]



[3] "For example, in one embodiment a laser etches a unique serial number, run number or a date stamp on the storage device during manufacturing. In another embodiment, however, storage device 151 contains a computer chip for electronically storing a unique identifier." Id. at col. 5, ll. 49-54.

If for some reason the storage manager is unable to read or retrieve the necessary security information in one of the blocks, the storage manager proceeds to block 216 and operates computer 100 in a restricted-access data storage mode. Id. at col. 5, ll. 15-19, 35-38, 42-46, 54-57. In restricted-access mode, removable media-drive 121 is configured "as a read-only drive such that the user can read data from the removable storage device but cannot write data to the drive. In addition, the user is prevented from accessing non-sensitive data within the organization." Id. at col. 7, ll. 9-13.

Otherwise, if the storage manager is able to retrieve or read the required security information, then "[i]n block 212, the storage manager generates a cryptographic key by combining the information, or a portion thereof, that was retrieved in blocks 206 through 210." Id. at col. 5, ll. 58-60. In one embodiment, "the storage manager combines, such as by concatenating, all or various portions of the information that was retrieved in blocks 206 through 210 and submits the result to a conventional cryptographic hashing algorithm." Id. at col. 6, ll. 4-8. When the storage manager is successfully able to complete method 200, computer 100 operates in full-access mode.

When the computer is operating in full-access mode, "storage management software uses a cryptographic key to encrypt and decrypt the data stream between the computer and the

removable storage device." Id. at col. 3, ll. 61-64. Depending upon the system's selected security level, the cryptographic key is generated by combining one or more of the following:

> (1) device-specific security information derived from the unique format information of the removable storage device, (2) manufacturing information that has been etched onto the storage device, (3) drive-specific information, such as drive calibration parameters, retrieved from the storage drive, and (4) user-specific information such as a password or biometric information.

Id. at col. 3, ll. 66 – col. 4, ll. 5. In addition to encrypting data written to the storage device, the computer allows the user to access the local area network and remote computer. Id. at col. 6, ll. 46-47. Thus, "[i]n this manner, the present invention allows storage device 151 to be used as an 'access card' by which the user gains access to sensitive data of the organization. In addition, data stored on other storage devices, such as internal hard disk 120 . . . may actually be encrypted using the unique key generated from the unique format information of key disk 151." Id. at col. 6, ll. 48-54.

LEGAL STANDARD

Claim construction is an issue of law for the court. Markman v. Westview Instruments, Inc., 517 U.S. 370, 372 (1996). Courts seek to give words of a claim their "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the

time of the invention." Phillips v. AWH Corp., 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc) (citations omitted). A person of ordinary skill in the art looks to "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." Id. at 1314 (quoting Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1116 (Fed. Cir. 2004)). "[T]he specification is the single best guide to the meaning of a disputed term," and is "thus, the primary basis for construing the claims." Id. at 1321 (citations and quotations omitted). However, a court should be careful not to import limitations from specific embodiments in the specification into the claims, see id. at 1320, nor should the construction of the claim exclude a preferred embodiment, see Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1583-84 (Fed. Cir. 1996).

The prosecution history "often inform[s] the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution." Phillips, 415 F.3d at 1317. The prosecution history "consists of the complete record of proceedings before the PTO," id., including a patent owner's statements during an inter partes review proceeding, see Aylus Networks, Inc. v. Apple Inc., 856 F.3d 1353, 1360 (Fed. Cir.

2017). This "ensure[s] that claims are not argued one way in order to maintain their patentability and in a different way against accused infringers." Id.

DISCUSSION

1. "detecting a storage device within a storage drive"

IV's Proposed Construction	Defendants' Proposed Construction
Detecting the presence of a storage device within a storage drive. • "storage device" – a device capable of storing computer data. • "storage drive" – hardware and software used to host and represent a storage device in a computer or computer system.	Determining that a removable storage device, such as a floppy diskette, has been inserted into a storage drive. • "storage device" – a device having a storage medium for holding digital information. • "storage drive" – a device suitable for servicing access requests for the storage device.

The parties dispute the meaning of the term "detecting a storage device within a storage drive." Defendants argue that this term requires a "removable" storage device, while IV argues that the claim term includes detecting both removable storage devices and fixed storage devices, like hard disk drives. At the hearing, the parties agreed that a "storage device" is "a device having a storage medium for holding digital information." Docket No. 250 at 39:17-40:8. The parties also dispute the meaning of the term "storage drive."

IV argues that because the term "removable" is not present in either claim 15 or 18, its inclusion would improperly import a limitation into the claim language. See JVW Enters., Inc. v. Interact Accessories, Inc., 424 F.3d 1324, 1335 (Fed. Cir. 2005) (holding a court should "not import limitations into claims from examples or embodiments appearing only in a patent's written description, even when a specification describes very specific embodiments of the invention or even describes only a single embodiment").

A court may depart from the plain and ordinary meaning of the claim language in only two instances: (1) if the patentee is acting as his own lexicographer, or (2) "when the patentee disavows the full scope of the claim term either in the specification or during prosecution." Hill-Rom Servs., Inc. v. Stryker Corp., 755 F.3d 1367, 1371 (Fed. Cir. 2014) (quoting Thorner v. Sony Comput. Entm't Am. LLC, 669 F.3d 1362, 1365 (Fed. Cir. 2012)). Neither party argues that the patentee is acting as his own lexicographer, but Defendants assert that the patentee disavowed detecting storage devices that are not removable. A court may find "disavowal or disclaimer based on clear and unmistakable statements by the patentee that limit the claims, such as 'the present invention includes . . .' or 'the present invention is . . .' or 'all embodiments of the present invention are . . . .'" Luminara Worldwide, LLC v. Liown Elecs.

Co., 814 F.3d 1343, 1353 (Fed. Cir. 2016). When a patent "describes the features of the 'present invention' as a whole, this description limits the scope of the invention." Regents of Univ. of Minn. v. AGA Med. Corp., 717 F.3d 929, 936 (Fed. Cir. 2013) (quoting Verizon Servs. Corp. v. Vonage Holdings Corp., 503 F.3d 1295, 1308 (Fed. Cir. 2007)).

Here, the specification states that: "the present invention allows storage device 151 to be used as an 'access card' by which the user gains access to sensitive data of the organization." '459 patent, col. 6, ll. 48-50. Since "[e]ach storage device 151 represents a removable storage device," the specification confirms that the invention involves a storage device that can be inserted into and removed from the computer, like an "access card." Id. at col. 3, ll. 8-9; see also id. at fig.1 (showing a computer system which depicts a removable device/drive combination).

In the specification, the patentee also distinguishes prior art, stating that "with conventional security measures it is very difficult to prevent an authorized user from appropriating sensitive data by simply copying the sensitive data to a removable storage device such as floppy diskette." Id. at col. 1, ll. 23-26. "According to the invention," this problem is "addressed by a secure computing environment in which a computer automatically operates in a secure 'full-access' data storage

mode when the computer detects the presence of a secure removable storage device. If the computer senses a non-secure removable storage device then the computer automatically operates in a 'restricted-access' mode." Id. at col. 1, ll. 3643 (emphasis added). While the term "storage device" is broad enough to include internal hard disk drives, the patentee has disavowed an invention that detects fixed as well as removable storage devices.

IV argues that the doctrine of claim differentiation requires that "removable" not be read into claims 15 and 18 because Defendants' construction would make the language of dependent claims 5, 28, 37, and 46 superfluous. "The doctrine of claim differentiation stems from the common sense notion that different words or phrases used in separate claims are presumed to indicate that the claims have different meanings and scope." Seachange Int'l, Inc. v. C-COR, Inc., 413 F.3d 1361, 1368–69 (Fed. Cir. 2005) (cleaned up). For example, dependent claim 28 recites: "The method of claim 18, wherein writing the encrypted digital data includes writing the encrypted digital data to a removable storage medium." '459 patent, claim 28. Claim 46 also recites, "[t]he computer of claim 39, wherein the storage device is a removable storage medium." Id. at claim 46. Thus, IV argues the storage device detected in claims 15 and 18 need not be removable.

Defendants respond that the "removable storage medium" in the claims is actually described in the specification as a subtype of a removable storage device. See id. at col. 7, ll. 43-65 (discussing the floppy diskette depicted in figures 3A and 3B as one embodiment of a storage device and the disc-shaped magnetic medium within it as a storage medium); see also id. at claim 16 ("The method of claim 15, wherein encrypting the digital data includes generating a cryptographic key as a function of format characteristics of an underlying storage medium of the storage device."). While the record is not clear about the difference between a "storage device" and a "storage medium," the use of different terms undermines IV's position that "removable" must not be included in claims 15 and 18. Therefore, "detecting a storage device within a storage drive" means "detecting a removable storage device within a storage drive."

The parties also dispute the meaning of "storage drive." Defendants, drawing from language in the specification, propose that a storage drive is "a device suitable for servicing access requests for the storage device." See id. at col. 3, ll. 13-14 ("Each removable media drive 121 represents a device suitable for servicing access requests for storage device 151 . . . ."). IV proposes that a storage drive is "hardware and software used to host and represent a storage device in a computer or computer

system." But this language does not appear in the claims, specification, or extrinsic evidence.

The claims require that a storage drive must be able to prevent or permit "write access" to a storage device depending on whether the removable storage device detected within it is secure. See id. at claim 18 (claiming a method for controlling access to a storage device comprising "configuring the storage drive to prevent write access . . . configuring the storage drive to permit write access"). The specification supports Defendants' reading of the claim language. The specification explains that "[e]ach removable media drive 121 represents a device suitable for servicing access requests for storage device 151 such as a floppy drive, a magneto-optical drive, a CD-ROM drive, a SuperDisk™ drive, a removable-cartridge drive such as a Zip™ drive, or even a tape drive." Id. at col. 3, ll. 13-17; see also id. at col. 3, ll. 7-8 ("[R]emovable media drives 121 . . . are used to access one or more removable storage devices 151.").

The parties agree that technical dictionaries from the time of the invention do not define "storage drive." However, dictionary definitions of "drive" and "disk drive" buttress Defendants' proposed construction. See Docket No. 258-1 (Ex. 18, The Authoritative Dictionary of IEEE Standards Terms (7th ed. 2000)) at 5 ("disk drive": "[a]n electromechanical device that reads from and writes to disks."); Docket No. 258-2 (Ex. 19, The

Computer Glossary (9th ed. 2001)) at 4 ("disk drive": "[a] peripheral storage device that holds, spins, reads and writes magnetic or optical disks. It may be a receptacle for disk cartridges, disk packs or floppy disks, or it may contain nonremovable disk platters like most personal computer hard disks."); Docket No. 258-3 (Ex. 20, The Computer Desktop Encyclopedia (2d ed. 1999)) at 5 (same); Docket No. 258-4 (Ex. 21, Microsoft Computer Dictionary (4th ed. 1999)) at 5 ("disk drive": "[a]n electromechanical device that reads from and writes to disks. . . . Two types of disk drives are in common use: floppy disk drives and hard disk drives."). Additionally, Defendants' proposed construction is supported by contemporaneous marketing literature from Imation, the original assignee of the '459 patent. A 1998 presentation given by Imation on its SuperDisk product (reference in the patent's specification) describes a "drive" as a component that can "[r]ead and write 120 MB superdisks." Docket No. 258-5 at 7.

In supplemental briefing, IV raises a new argument that a storage drive could be either a "logical drive" or a "physical drive." A "logical drive" is "[a]n allocated part of a physical disk drive that is designated and managed as an independent unit. For example, drives C:, D: and E: could represent three physical drives or one physical drive partitioned into three logical drives. Contrast with physical drive." Docket No. 259-2

(Ex. 1, The Computer Desktop Encyclopedia (2d. ed. 1999)) at 6. A "physical drive" is defined as "the actual unit of hardware of a disk or tape drive." Id. at 7. IV argues that a logical drive could be the storage drive because a storage device could be connected to a logical drive destination. However, IV provides no support -- intrinsic or extrinsic -- for this construction. Additionally, IV does not explain whether a logical drive can read from or write to a removable storage device. This last-minute proposed construction is incongruous with the rest of the claim language and specification. Accordingly, the Court declines the proposed construction and limits the term to a physical drive that can read from and write to a storage device. A "storage drive" is a "device suitable for servicing access requests for the storage device."

2. "sensing whether a storage device has device-specific security information" and "sensing whether the storage device has security information"

IV's Proposed Construction	Defendants' Proposed Construction
No construction required.	Determining whether the storage device has [devicespecific security information/security information] stored on it. This step requires sensing the presence of security information stored on the device, rather than sensing whether a password is required to access the device.

The parties dispute the meaning of the term "sensing whether the storage device has security information." '459 patent, claim 18. IV argues that the term does not require construction because it only requires the application of commonly understood words. Defendants urge the Court to interpret the word "has" to mean "stored on it."

The Court begins with the plain and ordinary meaning of the word "has," which means "to hold, include, or contain as a part or a whole." Docket No. 231-2 (Merriam-Webster's Collegiate Dictionary (10th ed. 1993)) at 5. This meaning is consistent with the position IV took during the two inter partes reviews of the '459 patent -- the first filed by Unified Patents, Inc., (IPR2016-01404) and the second by the Defendants (IPR2017-00467). During these proceedings, IV made several arguments about the scope of claims 15 and 18 in order to distinguish the cited prior art. The doctrine of prosecution disclaimer extends to inter partes review proceedings as long as a patent owner's statements are "clear and unmistakable." Aylus Networks, 856 F.3d at 1360-61.

To distinguish a prior art patent ("Blakley") during inter partes review, IV argued that the sensing limitation required the security information to be stored on the device for both claim 15 and claim 18. See Docket No. 231-3 at 20 ("Petitioners' argument ignores a key portion of the claim element -- that the

sensing action determines whether the device-specific security information is stored on the storage device. Petitioners' omission is not surprising because Blakley never stores the pseudorandom bit string on the storage device."); id. at 33 ("Petitioners' argument [for claim 18] fails because Blakley never discloses 'sensing whether the storage device has' the pseudorandom bit string. As explained above relative to claim 15, Petitioners conflate the pseudorandom bit string, which Blakley generates anew for each disk access and never stores, with the one-way function of the secret key, which is used for password authentication." (emphasis added)).

IV's argument was adopted by the PTAB in denying institution of inter partes review on claims 15 and 18. The Board noted that claim 15 "requires . . . a determination of whether the storage device contains 'device-specific security information.'" Docket No. 231-6 at 10 (emphasis added). It went on to find that "Blakley teaches [the] . . . pseudorandom bit string is not stored on the storage device, as required by claim 15." Id. at 12 (emphasis added). As to claim 18, the Board held that it also "requires a determination of whether the storage device contains 'security information.'" Id. at 13 (emphasis added). And it declined to institute review of claim 18 for the same reasons as claim 15. See id. at 14.

Therefore, the Court construes "sensing whether the storage device has security information" to mean "sensing whether the storage device contains security information stored on it." Defendants' also propose a limitation on what "sensing" requires. The Court gives the word "sensing" its plain and ordinary meaning.

3. "device-specific security information"

IV's Proposed Construction	Defendants' Proposed Construction
Information specific to a storage device that is used to secure information.	Information specific to the storage device (as opposed to manufacturing information that has been etched onto the storage device, drive-specific information, and user-specific information) that is used to secure access to the storage device.

The parties dispute the meaning of the term "device-specific security information." Both parties agree that device-specific information is information specific to a storage device. Defendants seek to construe the claim language to exclude "manufacturing information that has been etched onto the storage device, drive specific information, and user-specific information" from also being "device-specific security information," while IV argues that its construction is consistent with the construction adopted by the Patent Trial and Appeal Board ("PTAB") in a related inter partes review

proceeding. The parties also disagree about whether the security information is used to "secure information" or used to "secure access to the storage device."

The Court begins with the claim language. Claim 18 explicitly differentiates between "device-specific information associated with the storage device" and "user-specific information associated with a user." '459 patent, claim 18; see also Innova/Pure Water, 381 F.3d at 1119 ("[W]hen an applicant uses different terms in a claim it is permissible to infer that he intended his choice of different terms to reflect a differentiation in the meaning of those terms.").

The specification differentiates between the four types of security information. See, e.g., '459 patent, col. 3, ll. 64 – col. 4, ll. 5 (noting that depending upon the selected security level, the cryptographic key is generated by combining (1) device-specific security information, (2) manufacturing information, (3) drive-specific security information, and (4) user-specific security information). It also states that in one embodiment "the device specific security information can be combined with information that was etched into the storage device 151 via a laser during manufacturing," to increase the level of security of computer 100. Id. at col. 4, ll. 20-25.

During a prior inter partes review proceeding, IV argued:

> [T]he '459 patent consistently stresses that the "device-specific security information" is separate and distinct from other security information, including "(2) manufacturing information that has been etched onto the storage device, (3) drive-specific information, such as drive calibration parameters, retrieved from the storage device, and (4) userspecific information such as a password or biometic [sic] information."

Docket No. 231-4 at 21 (emphasis removed) (quoting '459 patent, col. 4, ll. 1-5). Because statements made by a patent owner during an inter partes review proceeding are part of the prosecution history, IV may not now argue that "device-specific security information" includes other types of security information.

IV asserts that its proposed construction is based on the PTAB's construction of the term. In a prior inter partes review proceeding, non-party UPI argued that "device-specific security information," meant "information that is specific to the storage device and used to secure access to the storage device." Docket No. 233-2 (Ex. A, IPR2016-01404, Final Written Decision) at 11. IV responded that the information was "unique," rather than specific. Id. The PTAB construed "device-specific security information" to mean "information particular to, but not necessarily unique to, a storage device used to secure access to the storage device." Id. at 12-13. The Court adopts the PTAB's definition, which is based on the plain and ordinary meaning of "specific," and holds that "device-specific security

information" means "information particular to, but not necessarily unique to, a storage device used to secure access to the storage device." Consistent with IV's prior statements to the PTAB, the Court also excludes from the construction the other three types of security information.

4. "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" / "the security information"

IV's Proposed Construction	Defendants' Proposed Construction
Information created by combining together devicespecific information and userspecific information for the purpose of securing access.	Information that is created by combining together (such as by concatenating) device-specific information and user-specific information and that is used to control access. This step requires more than using information falling under both categories.

At the hearing, the parties appeared to agree that the Court should use the plain and ordinary meaning of the term. See Docket No. 250 at 114:18-25. Consequently, the term "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" requires no further construction.

5. "encrypting digital data using the security information"

IV's Proposed Construction	Defendants' Proposed Construction
Using the security information to create an encrypted form of the digital data.	Using the security information to mathematically transform digital data into a secret, encoded form.

Both claims 15 and 18 describe "encrypting digital data using the security information." '459 patent, claims 15 and 18. The parties dispute what "encrypting" means. The Court gives the term its plain and ordinary meaning. See Docket No. 231-10 (Ex. 9, Newton's Telecom Dictionary (20th ed. 2004)) at 4 (describing "encryption" as "the transformation of data into a form unreadable by anyone without a secret decryption key"); Docket No. 231-11 (Ex. 10, McGraw-Hill Illustrated Telecom Dictionary (2001)) at 4 ("Encryption": "The process of translating of data into a secret code."); Docket No. 231-12 (Ex. 11, Dictionary of Computer and Internet Terms (7th ed. 2000)) at 4 ("encryption": "the act of converting information into a code or cipher so that people will be unable to read it."); Docket No. 231-13 (Ex. 12, Microsoft Press Computer Dictionary (3rd ed. 1997)) at 4 ("encryption": "The process of encoding data to prevent unauthorized access, especially during transmission. Encryption is usually based on a key that is essential for decoding."); Docket No. 231-14 (Ex. 13, The New Oxford American Dictionary (2d ed. 2005)) at 4 ("encrypt": "convert (information or data)

into cipher or code, esp. to prevent unauthorized access"); see also Docket No. 258-5 at 35 (Imation, the original assignee of the patent, describing "encryption" as "the scrambling of information to make it accessible only to specific parties . . . requir[ing] a key or password for access"). So, the term requires no further construction.

ORDER

For the reasons stated above, the Court construes the disputed terms as follows:

- "detecting a storage device within a storage drive" means "detecting a removable storage device within a storage drive"
    - o "storage device" is "a device having a storage medium for holding digital information"
    - o "storage drive" is "a device suitable for servicing access requests for a storage device"
- "sensing whether the storage device has security information" means "sensing whether the storage device contains security information stored on it"
- "device-specific security information" means "information particular to, but not necessarily unique to, a storage device used to secure access to the storage device (excluding manufacturing information, drive-specific information, and user-specific information)"

The terms "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" and

"encrypting digital data using the security information" do not require construction.

SO ORDERED.

/s/ PATTI B. SARIS
Patti B. Saris
Chief United States District Judge